TLE

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/077,851	02/20/2002	Marco Casassa Mont	1509-280	3203

7590 04/10/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 04/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/077,851	MONT ET AL.	
	Examiner	Art Unit	
	Thomas M. Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 January 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,6,9-11,13-15 and 20-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,6,9-11,13-15 and 20-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1,3,6,9-11,13-15 and 20-32 are pending.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

A method of exchanging a digital credential between a first computer node and a second computer node, the method comprising

- Establishing a secure connection between the first node and second node over a communication network;
- Prior to conducting a transaction between the first and second nodes, establishing trust or increasing the level of trust between the first and second nodes by
    - Transferring a digital credential from the first node to the second node over the secure connection;
    - Verifying the trustworthiness of the digital credential against at least one policy of the second node;

Upon a determination that the digital credential satisfies said at least one policy, conducting said transaction over the secure connection.

The word, "a" in the phrase "Prior to conducting a transaction between the first and second nodes," is indefinite because it has at least three meanings and it is uncertain whether the Applicant intended to claim a broader or stricter interpretation.

The first meaning is "Prior to conducting ***a*** transaction between the first and second nodes," where no prior transactions were performed between the first and second node, and prior to the ***"first"*** transaction between the first and second nodes, performing the steps of transferring and verifying the digital credential.

The second meaning is "Prior to conducting ***a*** transaction between the first and second nodes," where prior to conducting ***each and every transaction***, the step of transferring and verifying of the digital credential is performed.

The third meaning is "Prior to conducting ***a*** transaction between the first and second nodes," where prior to conducting any transaction, the step of transferring and verifying of the digital credential is sometimes performed, and sometimes not. However, as long as the steps of transferring and verifying the trustworthiness was ***performed prior to conducting at least one of transactions***, it would meet the recitation of the claim.

For purposes of examination, the Examiner has adopted the first meaning.

Response to Amendments

3. The Applicant has recited in amended claim 1, the limitation:

A method of exchanging a digital credential between a first computer node and a second computer node, the method comprising

- Establishing a secure connection between the first node and second node over a communication network;
- Prior to conducting a transaction between the first and second nodes, establishing trust or increasing the level of trust between the first and second nodes by
    - Transferring a digital credential from the first node to the second node over the secure connection;
    - Verifying the trustworthiness of the digital credential against at least one policy of the second node;
    - Upon a determination that the digital credential satisfies said at least one policy, conducting said transaction over the secure connection.

The Examiner notes that the transferring of the digital credential from the first to the second node may itself be considered a "transaction" between the first and second node. However, Applicant has clearly not interpreted the transferring of a digital credential to "count" as a transaction,

otherwise, the steps given in claim 1 would fail to meet its own limitation of "prior to conducting a transaction"

For this reason, the Examiner has interpreted steps which recite the transferring of a digital credential to not read upon the limitation "prior to conducting a transaction between the first and second nodes"

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1,3,9-11,13-15 and 20-32 are rejected under 35 U.S.C. 102(b) as being anticipated by Stefik et al., US patent 5629980.

In reference to claim 1:

Stefik (Figure 1) & (Column 7, lines 5-37) & (Col 6, lines 50-56) discloses a method of exchanging a digital credential between a first computer node and a second computer node, the method comprising

- Establishing a secure connection between the first node and second node over a communication network, where the secure connection is established between the repositories. (Column 27, lines 30-42) & (Column 7, lines 40-45)
- Prior to conducting a transaction between the first and second nodes, establishing trust or increasing the level of trust between the first and second nodes by
    - Transferring a digital credential from the first node to the second node over the secure connection, where the digital credential is the digital work which also contains the digital authorization (Column 7, lines 5-37) & (Column 7, lines 55-65)
    - Verifying the trustworthiness of the digital credential against at least one policy of the second node, where the digital credential is the digital work which also contains the digital authorization, and where the verification performed is a determination that all conditions associated with the rights condition are satified. (Column 7, lines 5-37) & (Column 7, lines 55-65)
- Upon a determination that the digital credential satisfies said at least one policy, conducting said transaction over the secure connection, where the transaction that takes place is the rendering of the digital content, and the policy that is satisfied is the digital rights which must be complied with to render the content (Column 18, lines 1-22) & (Column 49, lines 40-60) or install the software (Column 13, lines 30-41)

In reference to claim 3:

Stefik discloses a computer system according to claim 1, wherein the digital credential is an attribute credential of an entity at the first node, said entity being a user or a system or a service, where the digital credential is the usage rights to a work, and where the usage rights are an attribute credential of another entity, the system of the digital work. (Column 41, lines 45-57) & (Figure 10) & (Column 9, line 7 – Column 11, line 30, "Structure of a digital work") & (Column 6, lines 50-56)

Claims 9, 10 are substantially similar to claim 1 and is rejected for the same reasons. The processor structure is recited in (Column 14, lines 5-27)

Claim 11 is substantially similar to claim 23 and is rejected for the same reasons.

In reference to claim 13:

Stefik discloses a computer system according to claim 10, wherein the processors are further configured to perform the method of claim 20, and at least one of the first node and second node further comprises said graphical user interface. (Column 16, lines 42-67)

In reference to claim 14:

Stefik discloses a computer system according to claim 11, wherein the second node further comprises

- Said graphical user interface; (Column 16, lines 42-67) and

- A controller for allowing the user to change status of the digital credentials in real time where the controller for allowing the user to change is the keyboard. (Column 16, lines 42-67)

Claim 15 is substantially similar to claim 1 and is rejected for the same reasons.

In reference to claim 20:

Stefik discloses a method according to claim 1, further comprising

Presenting, via a graphical user interface and in human-readable format, to a user at either or both of said first and second nodes the digital credential transferred over the secure connection, where the human readable format is the digital rights grammar. (Figure 15) & (Column 7, lines 5-38) & (Column 16, lines 42-67)

In reference to claim 21:

Stefik discloses a method according to claim 20, wherein said presenting comprises displaying, by said graphical user interface, properties of said digital credential on a display, said properties comprising credential type, credential issuer, credential holder, and validity period, where the credential type is the type of the right(Figure 15, Item 1510, 1520, 1503, et seq.) , whether it be copying, printing, or distributing, where the credential issuer is the owner(Figure 15, Item 1525), where the validity period is the Time Spec(Figure 15, item 1512), and where the credential holder is the holder of the current authorization(Figure 15, Item 1516) or the ID of the rendering

device(Figure 15, Item 1504) and where the digital credential is presented to the user in the form of a digital rights grammar.

In reference to claim 22:

Stefik discloses a method according to claim 1, further comprising:

- Presenting, via a graphical user and in human-readable format, to a user at said first node a list of credentials of said user;
- Allowing the user to select at least one of the credentials from said list as the digital credential to be transferred over the secure.(Column 19, line 55 – Column 20, line 7)

In reference to claim 23:

Stefik discloses a method according to claim 1, further comprising:

- Establishing a plurality of secure connections between the second node and a plurality of said first nodes over the communication network, where the plurality of first nodes additionally include an authorization repository, and a master repository (Column 27, lines 5-56)
- Presenting, via a graphical user interface and in human-readable format, to a user at said second node a list of digital credentials which have been transferred over the respective secure connections and verified to be trustworthy, where the human-readable format is the rights grammar. (Figure 15) and the user interface (Column 16, lines 42-67)
- Allowing the user to monitor and intervene and on the credentials in real time, where the credentials and user rights change as the user uses or exercises the rights of the digital

work such as a copy count. (Column 36, lines 3-28) & (Column 24, lines 25-35) & (Column 25, lines 20 – Column 26, line 35)

In reference to claim 24:

Stefik (Figure 15) discloses a method according to claim 23, wherein said presenting comprises displaying, by said graphical user interface, properties of at least one of said credentials of the list on a display, said properties comprising credential issuer, credential holder, and validity period.

In reference to claim 25:

Stefik disclose a method according to claim 1, wherein said transaction comprises providing, over the secure connection, access by the first node to a service provided by the second node;

Said method further comprising

- Requesting by the first node, another digital credential from the second node; (Column 7, lines 5-37) & (Figure 1)
- Determining by the second node, whether the first node is entitled the receive the requested digital credential, and upon a positive determination, transmitting the requested digital credential from the second node to the first node over the secure connection. (Column 7, lines 5-37) & (Figure 1)

In reference to claim 26:

Stefik discloses a method according to claim 25, wherein said requesting, determining and transmitting are performed as part of said establishing trust or increasing the level of trust between the first and second nodes and are followed by

- Examining by the first node, the requested digital credential received from the second node prior to the transfer of the digital credential from the first node to the second node. (Column 7, lines 5-37) & (Figure 1)

In reference to claim 27:

Stefik discloses a method according to claim 25, wherein said requesting, determining and transmitting are performed after said establishing trust or increasing the level of trust between the first and second nodes and are followed by

- Using, by the first node, the requested digital credential received from the second node to establish trust or increase the level of trust between the first node and a third node which is coupled to said first node via the communication network and over another established secure connection, where the third node is the master repository. (Column 7, lines 5 – Column 8, line 20) & (Figure 2)

In reference to claim 28:

Stefik discloses a computer node according to claim 15, further comprising a credential validation server module executable by the processor for executing a two-phase control on the digital credential, said two phase control comprising:

- A first phase in which said credential validation server module interacts with at least one external entity to check if the digital credential is still valid, where a validation is determined with respect to time. (Column 7, lines 5-37) & (Column 21, line 45 – Column 22, line 30) & (Column 36, lines 3-28) & (Column 42, lines 5-21)
- A second phase in which said credential validation server module verifies the trustworthiness of the received digital credential against at least one policy by checking on at least one of the explicit constraints on the validation path, the issuer of the digital credential, and the context in which the digital credential has been issued, where the second phase is performed with respect to the policy which is the set of usage rights for the digital content that must be followed. (Column 7, lines 5-37)
- An additional two phase system for the transference of the digital work/rights is presented in (Column 34, lines 1-34)

In reference to claim 29:

Stefik disclose a computer node according to claim 28, further comprising an authorization server module executable by the processor for at least one of evaluating said at least one policy, modifying said at least one policy, and reloading the modified policy on the fly without service disruption, where the policies that must be followed are the rules set forth by the usage rights (Column 7, lines 5-37) & (Column 20, lines 38-50, 55-67)

In reference to claim 30:

Stefik discloses a computer node according to claim 29, further comprising a credential content management module executable by the processor for

- Abstracting the digital credential to be a collection of attributes independent of an original format of said digital credential, where the digital credentials are abstracted as a grammar which specify the digital rights, and where each of the attributes is independent in that each attribute controls a different right. (Figure 15) & (Column 17, "usage rights language" section, column 17, line 64 – Column 26,line 35)
- Returning the abstracted digital credential to the credential validation server module, where the digital credentials are verified or validated to determine if the rights are satisfied so that the digital content may be used. (Column 7, lines 5-37) & (Column 36, lines 3-28) & (Column 42, lines 5-21)

In reference to claim 31:

Stefik discloses a computer node according to claim 30, further comprising a user context manager module executable by the processor for

- Receiving the abstracted digital credential from the credential validation server module, and storing the abstracted digital credential in a user context area for an entire lifetime of said secure connection, where the digital credentials is the authorization containing the usage rights which are stored with the digital work. (Column 3, lines 50-61) & (Column 7, lines 5-37) & (Column 7, lines 55-65)

In reference to claim 32:

Stefik discloses a computer node according to claim 31, further comprising an object pool manager module executable by the processor for dynamically managing the content of multiple said user context areas stored by the user context manager module, wherein

- Said managing comprises at least one of modifying, adding, removing, and disabling one or more digital certificates stored in the user context areas, where the digital work may be deleted, and where the credential/digital certificate is a part of the digital work. (Column 25, lines 22-30) & (Column 7, lines 55-65) & (Column 23, lines 10-30) & (Column 11, lines 45-53)
- Said authorization server module accesses one or more of the user context areas and evaluates said at least one policy against the content of said one or more of the user context areas, where the policy that must be obeyed are the constraints of the usage rights. (Column 7, lines 5-37) & (Column 7, lines 55-65) & (Column 4, lines 13-24)

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stefik, US patent 5629980.

In reference to claim 6:

Stefik fails to explicitly disclose a method according to claim 1, wherein the digital credential is an identity certificate of a user.

However, the use of identity certificates of users are well known in the art. For Example, Stefik employs them as another digital credential to be used to help established the identity of the repository, and hence, the user of the repository (Column 27, line 30 – Column 28, line 31) & (Column 13, lines 59-67)

Stefik furthermore discloses that the authorizations (Column 22, lines 57-67) themselves use certificates. (Column 41, lines 40-57)

It would have been obvious to one of ordinary skill in the art at the time of invention to have the digital credential be an identity certificate of user in order to use a well known method which allows the user be properly authenticated, and the user may be properly assigned the privileges associated with his or her digital identity.

Conclusion

8. The following art not relied upon is made of record:

- US patent 6609198 discloses a method of logon service providing credential level change without a break in the session
- US patent 5164988 discloses a method of using a private certification key
- US patent 5757920 discloses a method of logon certification

9. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of the final action and the advisory action is not mailed under after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension pursuant to 37 CFR 1.136(A) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (571)272-3838.

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist	Telephone: 571-272-2100	Fax: 703-872-9306
Customer Service Representative	Telephone: 571-272-2100	Fax: 703-872-9306

TMH

March 31st, 2006